IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

In re Benefits Partner, LLC d/b/a Salus Group Litigation	Case No.: 2:25-cv-11108 Hon. Linda V. Parker **CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Janine Orosco, Arthur Wagner, Preston Tilger, and John Stacho ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint ("Complaint") against Defendant Benefits Partner, LLC d/b/a Salus Group ("Defendant" or "Benefits Partner"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

I. NATURE OF THE ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant Benefits Partner failed to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") and protected health information ("PHI"), collectively, "Private Information".[1]

3. According to Benefits Partner, on October 9, 2024, it "identified suspicious activity in one employee's email account."[2] As a result, Benefits Partner launched an investigation to determine the nature of the event. *Id.* Defendant employed a third-party forensic firm to conduct an investigation, which determined that certain files containing Private Information were accessed and/or acquired by an unauthorized party, *id.*, causing widespread injuries to Plaintiffs and Class Members (the "Data Breach").

4. According to Defendant's Notice, Defendant spent more than four months analyzing the data. *See id.* (compromise discovered on October 9, 2024, and analysis completed in late February 2025). The ensuing investigation revealed that during the data security event, the Private Information of the Class was compromised, including emails and/or attachments of the Class were accessed from Defendant's network. *Id.*

---

[1] *See* https://thesalusgroup.com/security-incident/ (last visited June 9, 2025).
[2] *See id.*; *see also* Notice of Data Breach, Benefits Partner dba Salus Group, MASS.GOV, https://www.mass.gov/doc/2025-612-benefits-partner-llc/download (last visited June 9, 2025).

5. The Notice of the Data Breach obfuscates the nature of the Data Breach and the threat it posed. The Notice fails to disclose who exactly was impacted, how many people were impacted, how the Data Breach happened, exactly what information was compromised, or when the Data Breach actually occurred.

6. Although the Data Breach took place before October 9, 2024, Benefits Partner waited 169 days, or until March 27, 2025, before it finally began notifying employers and insurance carriers about the Data Breach.

7. And Defendant waited approximately one half of a year before it finally began to notify affected individuals that their Private Information was compromised.

8. In letters dated April 7, 2025, Plaintiffs Stacho, Wager, and Orosco received Notice of the Data Breach.[3] In a letter dated April 25, 2025, Plaintiff Tilger received Notice of the Data Breach.[4] Plaintiff Orosco also received their Notice Letters on or around April 15, 2025.

9. Such delayed notice diminished Plaintiffs' and Class Members' ability to timely and thoroughly mitigate and address the increased, imminent risk of identity theft and other harms the Data Breach caused. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of their PII/PHI misuse.

---

[3] *See* Exhibit A, Stacho Notice Letter; Exhibit B, Wagner Notice Letter; Exhibit C, Orosco Notice Letter.

[4] *See* Exhibit D, Tilger Notice Letter.

10. While the Private Information impacted varies depending on the individual, the type of Private Information potentially exposed includes names, Social Security numbers, dates of birth, driver's license numbers, financial account information, as well as PHI including information related to clinical treatment and health insurance. Based on the breach notice sent to Massachusetts residents, Benefits Partner is providing affected individuals with a list of the specific types of sensitive information impacted.[5]

11. Plaintiff Stacho, for example, was informed that his "name, date of birth, Social Security number, health insurance information, and/or clinical or treatment information" were compromised and potentially accessed by an unauthorized party.[6]

12. Plaintiff Wagner, for further example, was informed that his "name, date of birth, Social Security number, and/or health insurance information was compromised and potentially accessed by an unauthorized party.[7]

13. Plaintiff Orosco was informed that his name, date of birth, and Social Security number.[8]

---

[5] *See* https://www.mass.gov/doc/2025-612-benefits-partner-llc/download (last visited June 9, 2025).
[6] Exhibit A, Stacho Notice.
[7] Exhibit B, Wagner Notice.
[8] Exhibit C, Orasco Notice.

14. Plaintiff Tilger was informed that his "name, date of birth, and Social Security number" were impacted.[9]

15. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

16. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

17. In failing to adequately protect the Private Information of individuals whose Private Information was in Defendant's custody and control, by failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of individuals.

18. Plaintiffs and the Class are victims of Defendant's negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their Private Information. But Defendant betrayed that trust when Defendant failed to properly use industry-standard security practices to prevent the Data Breach.

19. Benefits Partner is a healthcare solutions provider specializing in employee benefits and wellness programs for organizations across various

[9] Exhibit D, Tilger Notice.

industries. Defendant assists with benefits consulting, brokerage, and administration.[10]

20. Defendant obtains the Private Information of Plaintiffs and Class Members from their current and former employees and/or insurance carriers in connection with the services provided by Defendant. Thus, Plaintiffs and the Class were required to entrust Defendant with their sensitive, non-public Private Information. Defendant could not perform its operations or provide its services without collecting Plaintiffs' and Class Members' Private Information and retains it for many years, at least, even after the relationship has ended.

21. Businesses like Defendant that handle Private Information owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their personal information.

[10] https://thesalusgroup.com/ (last visited June 9, 2025).

22. Defendant breached these duties owed to Plaintiffs and Class Members by failing to safeguard their Private Information it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, and such failures allowed criminal hackers to access and steal Private Information from Defendant's care.

23. Plaintiffs and Class Members allege that Defendant failed to implement adequate cybersecurity measures, failed to train employees in information security, failed to encrypt or redact Private Information, and failed to monitor and protect its network from foreseeable threats—rendering its systems vulnerable to attack.

24. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to protect the sensitive data of the Class.

25. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure Private Information left it in a dangerous condition.

26. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information from Defendant's network because of the data's value in exploiting and stealing identities. As a direct and proximate result of Defendants' inadequate data security and breaches of its duties to handle Private Information with reasonable

care, Plaintiffs' and Class Members' Private Information has been accessed by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

27. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud. Cybercriminals value PII and PHI because it enables them to commit identity theft, open fraudulent accounts, file false insurance claims, and impersonate victims for financial gain. The stolen data in this case remains in the hands of criminals, and Plaintiffs and Class Members remain at risk for ongoing and future identity theft.

28. The exposure of Plaintiffs' and Class Members' Private Information is permanent—this "bell cannot be unrung." The data will never again be private, and the risk of future misuse is substantial and enduring.

29. The exposure of an individual's Private Information due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

30. As a result of the Data Breach, Plaintiffs' and Class Members suffered and will continue to suffer concrete injuries in fact, including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake adequate measures to protect the data it collects and maintains.

31. To recover from Defendant for these harms, Plaintiffs, on their own behalf and on behalf of the Class as defined herein, brings claims for negligence, negligence per se, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of third-party beneficiary contract, invasion of privacy, breach of confidence, and for declaratory judgment to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information in its care.

32. Plaintiffs and Class Members seek damages and equitable relief requiring Defendant to (a) disclose the full nature of the Data Breach and types of

Private Information exposed; (b) implement data security practices to reasonably guard against future breaches; (c) provide, at Defendant's expense, all Data Breach victims with lifetime identity theft protection services; and (d) compensatory damages and reimbursement for out-of-pocket costs.

II. PARTIES

33. Plaintiff Janine Orosco is a resident and citizen of Jackson, Michigan.

34. Plaintiff John Stacho is a resident and citizen of Rochester Hills, Michigan.

35. Plaintiff Preston Tilger is a resident and citizen of Rives Junction, Michigan.

36. Plaintiff Arthur Wagner is a resident and citizen of Seattle, Washington.

37. Defendant Benefits Partner, LLC, dba Salus Group is a Michigan limited liability company with its headquarters and principal place of business located at 38233 Mound Rd, Building F, Sterling Heights, Michigan 48310.

III. JURISDICTION AND VENUE

38. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the

proposed Class, including Plaintiffs, are citizens of states different from Defendant, as the Data Breach affected Class Members in multiple states.

39. This Court has general personal jurisdiction over Defendant because Defendant is organized under the laws of Michigan, is registered to do business in Michigan, and maintains its principal place of business in Michigan. Defendant has purposefully availed itself of the privileges of conducting business in this District, making the exercise of jurisdiction by this Court appropriate and proper.

40. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1)–(b)(2) because Defendant maintains its principal place of business in this District, and a substantial part of the events or omissions giving rise to the claims occurred in this District. Defendant is based in this District, stores Plaintiffs' and Class Members' Private Information here, and caused harm to Plaintiffs and Class Members from and/or within this District.

IV. FACTUAL BACKGROUND

A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for Private Information That It Collected and Maintained.

41. Defendant is a Michigan based healthcare solutions provider specializing in employee benefits and wellness programs for organizations across

various industries. Defendant serves a diverse range of clients nationwide, including school districts, construction firms, physician groups, and various associations.[11]

42. Defendant obtains the Private Information of Plaintiffs and Class Members from their current and former employees and/or insurance carriers in connection with the services provided by Defendant.

43. As a condition and in exchange for Defendant providing services on behalf of Plaintiffs and the Class, Plaintiffs and Class Members were required to entrust Defendant with highly sensitive Private Information, including, for each, their full name, date of birth, Social Security number, health insurance information, and other sensitive data.

44. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

45. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive Private Information belonging to Plaintiffs and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

46. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of

[11] *Id.*

identity theft and fraud for the individuals whose Private Information was compromised.

47. Upon information and belief, Defendant made promises and representations—through its privacy policy and other disclosures required by applicable federal and state privacy laws and industry standards, including but not limited to HIPAA where applicable—to its clients, including the employers of Plaintiffs and Class Members. These representations included that any Private Information collected would be kept secure and confidential, that the privacy of such information would be maintained, and that any sensitive data would be deleted once it was no longer required. Indeed, Defendant's privacy policy states that it "is committed to securing your data and keeping it confidential."[12]

48. Plaintiffs and Class Members relied on these promises from Defendant, a sophisticated business entity and provider of services related to healthcare, to implement reasonable practices to keep their sensitive Private Information confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete Private Information from Defendant's systems when no longer necessary for its legitimate business purposes.

[12] *Privacy Policy*, SALUS GROUP, https://thesalusgroup.com/privacy-policy (last visited June 9, 2025).

49. But for Defendant's promises to keep Plaintiffs' and Class Members' Private Information secure and confidential, Plaintiffs and Class Members would not have entrusted their Private Information to Defendant.

50. Consumers in general demand security to safeguard their Private Information, especially when sensitive financial information is involved. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[13] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[14]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[15]

c. 89% of consumers stated that "I care about data privacy."[16]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[17]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[18]

---

[13] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited June 9, 2025).
[14] *Id*. at 3.
[15] *Id*.
[16] *Id*. at 9.
[17] *Id*.
[18] *Id*.

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[19]

51. Based on the foregoing representations and warranties, Plaintiffs and Class Members entrusted their Private Information to Defendant, as part of an employment and/or insurance relationship, with the reasonable expectation and mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

52. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information. To that end, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

53. Defendant derived economic benefits from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its operations or furnish the services it provides.

54. By obtaining, using, and benefiting from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and

[19] *Id*. at 11.

knew or should have known that it was responsible for protecting that Private Information from unauthorized access and disclosure.

55. Defendant had and has a duty to adopt reasonable measures to keep Plaintiffs' and Class Members' Private Information confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks, and train employees with access to use adequate cybersecurity measures.

56. Additionally, Defendant had and has obligations created by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), common law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure. Defendant failed to do so.

B. Defendant Failed to Adequately Safeguard Plaintiffs' and Class Members' Private Information, Resulting in The Data Breach

57. On or about April 7, 2025 Defendant began sending Plaintiffs and other Data Breach victims letters informing them of the Data Breach ("Notice Letters").

58. The Notice Letters generally inform as follows, in part:

> In October, we identified suspicious activity in one employee's email account. We immediately disabled the account, reset the employee's password, and began an investigation with assistance from a third-party forensic firm. Through the investigation, we determined that there was unauthorized access to the account for a period of time on October 9, 2024. The investigation was unable to

> determine which emails, if any, were viewed by the unauthorized person. Accordingly, we conducted a comprehensive review of the contents of the email account. This review included identifying emails and attachments with personal information; cataloging the information; determining our relationship with each identified individual; and determining from whom we received the information.
>
> We completed our analysis of the data involved in late February 2025 and began informing employers and insurance carriers of the incident on or around March 27, 2025. The information involved varied by individual but generally included names, dates of birth, Social Security numbers, drivers' license numbers, financial account information, health insurance information, and/or clinical or treatment information.[20]

59. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

60. Thus, Defendant's purported "disclosure" amounts to no meaningful disclosure at all, as it fails to provide Plaintiffs and Class Members with any specific information about the critical facts of the Data Breach. Without these details, Plaintiffs' and Class Members' ability to mitigate the resulting harm is significantly

[20] https://thesalusgroup.com/security-incident/ (last visited June 9, 2025). *See also* Exhibit A, Stacho Notice.

impaired. The Notice Letters also failed to clarify who the breach affected; how many individuals were impacted; or what specific categories of information were compromised. These omissions leave Plaintiffs and Class Members unable to fully understand the scope of the threat they now face.

61. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[21] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[22]

62. Defendant's notice to HHS was dated April 8, 2025—six months after the Data Breach occurred. According to the online notice, the breach affected 40,177 individuals.[23]

---

[21] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed March 11, 2025) (emphasis added).

[22] *Id.*

[23] HHS Office for Civil Rights, Cases Currently Under Investigation, report dated April 8, 2025, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* June 9, 2025).

63. Similarly, although the Data Breach occurred on or around October 9, 2024, Defendant waited until on or around April 7, 2025, before notifying the public or affected individuals about it, diminishing Plaintiffs' and Class Members' ability to timely and thoroughly mitigate and address harms resulting from their Private Information's unauthorized disclosure.[24]

64. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, providing monitoring services, and advising Plaintiffs "it is always a good idea to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." *Id.*

65. Defendant's response to the breach consisted primarily of providing its employees with additional training on avoiding suspicious emails and vaguely asserting that it implemented "additional security controls" in its email environment.[25]

66. Defendant's offer of short-term credit monitoring fails to adequately address this enduring threat. Furthermore, Defendant has not committed to long-term mitigation or compensation for the victims' losses.

[24] *See* Exhibit A, Stacho Notice.
[25] https://thesalusgroup.com/security-incident/ (last visited Apr. 14, 2025).

67. These minimal steps are an acknowledgment that Defendant had inadequate security protocols in place prior to the Data Breach. The vague nature of these remedial steps further demonstrates Defendant's failure to adopt and disclose meaningful, concrete corrective measures.

68. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive Private Information it collected and maintained from Plaintiffs and Class Members, such as MFA, standard monitoring and altering techniques, encryption, or deletion of information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network and exfiltrate files containing Plaintiffs' and Class Member's Private Information.

69. Plaintiffs' and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiffs' and Class Members' Private Information from Defendant's network systems, where they were kept without adequate safeguards and in unencrypted form.

70. Cybercriminals often compile stolen information like that taken in the Data Breach into comprehensive identity packages known as "Fullz," which can be sold or used to commit extensive financial fraud, medical identity theft, and other crimes.

71. On information and belief, Plaintiffs' and Class Members' Private Information has already been, or will imminently be, uploaded to illicit marketplaces on the dark web for sale and exploitation by cybercriminals.

72. The sensitive nature of the compromised information—particularly Social Security numbers, which cannot be changed—means that Plaintiffs and Class Members face a lifelong risk of identity theft and fraud.

C. Defendant Failed to Adequately Prevent the Data Breach

73. Defendant could have prevented the Data Breach by implementing basic and reasonable cybersecurity measures, including properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' Private Information, limiting access to sensitive data, requiring multifactor authentication ("MFA"), conducting regular password resets, training personnel on cybersecurity best practices, and implementing adequate logging and alerting systems to detect unauthorized access. However, Defendant failed to take these precautions.

74. Defendant also failed to follow basic and widely recommended technical safeguards issued by the Federal Bureau of Investigation ("FBI") and Microsoft Threat Intelligence. The FBI has repeatedly emphasized that "[p]revention

is the most effective defense against ransomware and it is critical to take precautions for protection."[26]

75. Specifically, the FBI recommends that entities like Defendant implement: (i) awareness and training programs to educate end users on ransomware; (ii) strong spam filters and email authentication tools such as SPF, DKIM, and DMARC; (iii) scanning of incoming and outgoing emails to block threats; (iv) firewall rules to block access to known malicious IP addresses; (v) disabling macro scripts in documents received via email; (vi) Software Restriction Policies (SRP) to block unauthorized execution from common ransomware locations; (vii) application whitelisting; (viii) virtualized environments for risky operations; (ix) categorization of data based on value; and (x) segmentation of networks and data by organizational unit.[27]

76. The Microsoft Threat Protection Intelligence Team also recommends several key preventive measures, including: applying all security updates promptly; auditing and removing privileged credentials; treating commodity malware alerts as full compromises; ensuring collaboration across IT, security operations, and system administration teams; building strong credential hygiene by using just-in-time

---

[26] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed June 9, 2025).
[27] *Id.* at 3-4.

administrative credentials and multifactor authentication; and hardening infrastructure with features like Windows Defender Firewall, tamper protection, cloud-delivered protection, and attack surface reduction rules.[28]

77. Had Defendant implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate malicious activity in Defendant's network systems for the period it took to carry out the Data Breach, including the reconnaissance necessary to identify where Defendant stored Private Information, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

78. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

79. Defendant's failure to implement widely recognized cybersecurity safeguards—despite specific guidance from the FBI and Microsoft—left its systems

[28] *See* Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

exposed to unauthorized access. Had Defendant adopted these industry-standard practices, the Data Breach likely would have been prevented.

80. This failure not only reflects a serious departure from reasonable security expectations, but also underscores Defendant's tortious conduct and breach of contractual obligations. Defendant did not detect the intrusion until after cybercriminals had accessed Plaintiffs' and Class Members' Private Information, demonstrating that it lacked any effective mechanisms to monitor for, detect, or respond to cyberattacks in a timely manner.

D. Defendant Knew of the Risk of a Cyberattack Because Private Information Remains High Value to Criminals

81. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[29] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[30]

[29] 17 C.F.R. § 248.201 (2013).
[30] *Id.*

82. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[31]

83. For example, Personal Information can be sold at a price ranging from $40 to $200.[32] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[33]

84. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3)

---

[31] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 9, 2025).

[32] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 9, 2025).

[33] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 9, 2025).

Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

85. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

86. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

87. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[34] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[35] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[36]

88. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[37] Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[38]

---

[34] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed June 9, 2025).
[35] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed June 9, 2025).
[36] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed June 9, 2025).
[37] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited June 9, 2025).
[38] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited December 11, 2024).

89. Healthcare data is especially prized by data thieves. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[39]

90. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[40]

91. A study by Experian, a credit monitoring service, found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[41] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of

[39] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited June 9, 2025).
[40] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed June 9, 2025).
[41] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed June 9, 2025).

medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[42]

92. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers and names.

93. In recent years, the medical services industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

94. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

---

[42] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed June 9, 2025).

E. Defendant Knew of the Risk of a Cyberattack Because Businesses in Possession of Private Information Are Particularly Susceptible

95. Defendant's negligence in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

96. Private Information of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the dark web.

97. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

98. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

99. Data thieves regularly target entities in industries like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after

by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

100. Defendant knew or should have known of the heightened risk of cyberattacks, particularly because insurance entities in possession of sensitive Private Information are prime targets for hackers.

101. Data breaches affecting insurance companies have become widespread, underscoring the heightened duty to maintain robust security safeguards.

102. Defendant's obligations were further magnified by the increasing reliance on electronic systems to store confidential personal data, making the risk of data compromise foreseeable and preventable.

103. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[43] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[44]

[43] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last accessed June 9, 2025).
[44] *Id.*, at 15.

104. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[45]

105. Additionally, as companies became more dependent on computer systems to run their business,[46] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[47]

106. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including

---

[45] https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection.

[46] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[47] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[48]

107. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

108. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable employee service provider, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

109. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68

[48] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed June 9, 2025).

percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[49]

110. In 2023, a record 3,205 data compromises were reported, affecting over 353 million individuals—a 78% increase from 2022. Notably, 25.2% of these breaches occurred in the healthcare and medical sectors, underscoring the heightened vulnerability of sensitive information held by companies like Defendant. In the years leading up to the breach, several high-profile healthcare-related data breaches occurred, including HCA Healthcare (11M records, July 2023), Managed Care of North America (8M, March 2023), PharMerica (5M, March 2023), HealthEC (4M, July 2023), ESO Solutions (2.7M, September 2023), and Prospect Medical Holdings (1.3M, July–August 2023).

111. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[50] These incidents

---

[49] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited June 9, 2025).

[50] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter. org/publication/2024-data-breach-report/ (last visited June 9, 2025).

should have placed Defendant on heightened notice of its duty to implement robust data protection measures.

112. However, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being wrongfully disclosed to cybercriminals.

113. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

114. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

115. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

116. Accordingly, as an insurance entity in custody of the Private Information of its customers, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

F. Defendant Failed to Comply with The Required FTC Rules And Guidance

117. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

118. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[51]

119. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[52]

120. The FTC emphasizes that immediate notification of a data breach is critical so that those impacted can take measures to protect themselves from fraud, identity theft, and other harm.[53]

121. The FTC further recommends that companies not maintain confidential personal information, like Private Information, longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[51] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 14, 2025).
[52] *Id.*
[53] *Id.*

122. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

123. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

124. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

125. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[54]

126. In violation of its duties under the FTC Act, Defendant failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to detect or respond to a breach in a timely manner. Defendant was fully aware of its obligation to protect the Private Information it collected and the significant risk to Plaintiffs and Class Members if it failed to do so. Defendant's conduct was particularly unreasonable given the volume and sensitivity of the Private Information is stored and the foreseeable consequences of a data breach.

127. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

---

[54] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last viewed June 9, 2025).

G. Defendant Failed to Comply with HIPAA Guidelines

128. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

129. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[55] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

130. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

131. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

[55] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

132. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

133. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

134. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

135. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

136. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

137. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[56]

138. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

139. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

---

[56] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last viewed June 9, 2025) (emphasis added).

140. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[57] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[58]

H. Defendant Failed to Comply with Industry Standards

141. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

---

[57] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last viewed June 9, 2025).

[58] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last viewed June 9, 2025).

142. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[59]

143. The NIST also recommends certain practices to safeguard systems[60]:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

---

[59] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last viewed June 9, 2025).

[60] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist- framework (last viewed June 9, 2025).

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

144. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software

and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[61]

145. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

86. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points; strong passwords; multi-layer security, including firewalls,

[61] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last viewed June 9, 2025).

anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data; A properly trained helpdesk equipped to recognize and respond to social engineering attacks is also a critical component of any effective cybersecurity program.

146. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

I. Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard Their Private Information

147. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

148. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private

Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

149. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner and act upon data security warnings and alerts in a timely fashion.

150. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

151. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

152. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

J. Plaintiffs and Class Members Suffered Common Injuries and Damages Due to Defendant's Conduct

153. Defendant's failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' Private Information directly and proximately injured Plaintiffs and Class Members by the resulting disclosure of their Private Information in the Data Breach.

154. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen – particularly Social Security numbers and PHI – fraudulent use of that information and damage to victims may continue for years.

155. Plaintiffs and Class Members are also at a continued risk because their Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect the Private Information of individuals to whom it provides services.

156. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their Private Information ending up in criminals' possession, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy and theft of their Private Information; (b) out-of-pocket expenses and financial losses related to identity theft, fraud prevention, credit monitoring, and remediation; (c) lost time and productivity spent addressing the breach and mitigating identity theft, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) emotional

distress, including anxiety, stress, sleep disruption, and fear caused by the breach; (e) loss of the opportunity to control how their Private Information is used; (f) loss of the benefit of their bargain with Defendant; (g) increased spam and unwanted communications; (h) lost opportunity costs, including delayed tax refunds and wages; (j) deprivation of the value and control of their Private Information, including its unauthorized use, publication, and continued risk of disclosure due to Defendant's ongoing failure to secure it.

i. The risk of identity theft to Plaintiffs and the Class is present and ongoing

157. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach, especially because Defendant's failures resulted in Plaintiffs' and Class Members' PII and PHI falling into the hands of identity thieves.

158. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[62] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued

[62] 17 C.F.R. § 248.201 (2013).

driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[63]

159. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

160. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.

---

[63] *Id.*

161. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

162. As stated prior, on information and belief, in the Data Breach, cybercriminals were able to access the Plaintiffs' and the Class's Private Information, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages. Once an individual's Private Information is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[64]

163. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[65] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is

[64] Ryan Toohil, *What do Hackers do with Stolen Information*, Aura, (Sept. 5, 2023) https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited February 18, 2025).
[65] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last viewed June 9, 2025).

ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[66] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

164. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[67] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[68] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[69]

165. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers.

---

[66] *Id.*
[67] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[68] *Id.*
[69] *Id.*

Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

166. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[70] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[71]

167. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' Private Information.

168. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier

[70] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 9, 2025).
[71] *Id.*

it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

169. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

170. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[72]

[72] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

171. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[73]

172. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

173. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such

[73] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited June 9, 2025).

as emails, driver's license numbers, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

174. What's more, theft of PII and PHI is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII and PHI are valuable property rights.

175. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

176. Where the most PII and PHI belonging to Plaintiffs and Class Members was accessible from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning that Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

177. Further, there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.[74]

178. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial and credit accounts for many years to come.

179. Accordingly, the Data Breach has caused Plaintiffs and the Class to be at a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein.

180. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur and strengthened its data systems accordingly.

ii. Financial losses due to the data breach

[74] U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

181. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[75]

182. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[76]

183. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for

---

[75] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited June 9, 2025).

[76] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited June 9, 2025).

good."[77] Yet, Defendant failed to rapidly report to Plaintiffs and the Class that their Private Information was stolen.

184. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

185. For instance, identity thieves use stolen Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

186. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [78] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[79]

---

[77] *Id.*
[78] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[79] *Id.*

187. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:[80]

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

188. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[81] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[82]

189. Identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being

---

[80] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 9, 2025).
[81] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited June 9, 2025).
[82] *See* https://www.investopedia.com/terms/s/ssn.asp (last visited June 9, 2025).

issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

190. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

191. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

192. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number,

so all of that old bad information is quickly inherited into the new Social Security number."[83]

193. The California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[84]

194. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[85] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical

---

[83] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 9, 2025).

[84] *See* https://oag.ca.gov/idtheft/facts/your-ssn (last visited June 9, 2025).

[85] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited June 9, 2025).

maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

195. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated."

196. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

197. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

iii. Loss of time to mitigate the risk of identity theft and fraud.

198. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

199. Defendant's failure to properly notify Plaintiffs and the Class of the Data Breach exacerbated Plaintiffs' and the Class's injuries by depriving them of the earliest opportunity to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach

200. Plaintiffs and Class Members were compelled to spend time mitigating the risk of harm—particularly due to the exposure of their Social Security numbers and other government IDs—not to manufacture injury, but to take necessary steps prompted by the nature of the Data Breach and Defendant's guidance.

201. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit

reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

202. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[86]

203. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[87]

204. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these

[86] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[87] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited June 5, 2025).

heightened measures for years, and possibly their entire lives, because of Defendant's conduct that caused the Data Breach.

iv. Diminished value of private information

205. Personal data like Private Information is a valuable property right.[88] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

206. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[89] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[90, 91] Consumers who

[88] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[89] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last viewed June 9, 2025).

[90] https://datacoup.com/ (last viewed June 9, 2025).

[91] https://digi.me/what-is-digime/ (last viewed June 9, 2025).

agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[92]

207. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[93]

208. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

209. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

v. ***Future cost of credit and identity theft monitoring is reasonable and necessary***

210. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

---

[92] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last viewed June 9, 2025).

[93] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited June 9, 2025).

211. Defendant disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

212. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered due to the Data Breach.

213. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals

participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

214. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

215. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[94] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

216. The actual and adverse effects to Plaintiffs and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require

[94] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

Plaintiffs and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

217. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

218. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

219. Consequently, Plaintiffs and Class Members are at present and ongoing risk of fraud and identity theft for many years into the future.

vi. Loss of benefit of the bargain

220. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

221. When agreeing to provide their Private Information, Plaintiffs and Class Members, as part of an employment and/or insurance relationship, understood and expected that Defendant maintained adequate data security to protect the Private Information they were required to provide.

222. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services of less value than what they expected to receive under the bargains struck with Defendant.

K. Plaintiffs' Experiences

i. Plaintiff Janine Orosco

223. Plaintiff Janine Orosco was required to provide her employer with her Private Information as a condition of employment. Upon information and belief, Plaintiff Orosco's Private Information was and continues to be stored and maintained in Defendant's network systems through this provision of her Private Information.

224. Plaintiff Orosco greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Orosco diligently protects her Private Information and stores any documents containing Private Information in a

safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

225. Plaintiff Orosco would not have entrusted her Private Information to her employer had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

226. At the time of the Data Breach Defendant retained Plaintiff Orosco's Private Information in its network systems with inadequate data security, causing Plaintiff Orosco's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

227. On April 7, 2025, Plaintiff Orosco received Defendant's Notice Letter informing that her Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Orosco's sensitive Private Information, including her full name, date of birth, and Social Security number.

228. Plaintiff Orosco has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Orosco now monitors her financial and credit statements multiple times a week and has spent hours dealing

with the Data Breach, valuable time she otherwise would have spent on other activities.

229. Plaintiff Orosco further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Orosco is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

230. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Orosco's and Class Members' Private Information was targeted, accessed, and misused, including through publication and dissemination on the dark web.

231. Plaintiff Orosco further believes her Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

232. The Data Breach has also caused Plaintiff Orosco to suffer fear, anxiety, and stress about her Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Defendant still has not fully informed her of key details about the Data Breach's occurrence or the information stolen. As an employee of a client of Defendant, Plaintiff Orosco reasonably believes she is at

a higher risk of fraud, and to suffer occupational and financial impact as a result of that fraud.

233. Moreover, since the Data Breach Plaintiff Orosco has experienced suspicious spam calls using her Private Information compromised in the Data Breach, and believes this to be an attempt to secure additional information from or about her.

234. As a direct and traceable result of the Data Breach, Plaintiff Orosco suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Orosco and (g) other economic and non-economic harm.

ii. Plaintiff John Stacho's Experiences

235. As a condition of providing services on behalf of Plaintiff John Stacho, Defendant obtained Plaintiff Stacho's Private Information—including name, Social Security number, date of birth, health insurance information, and/or clinical or treatment information.

236. Defendant was in possession of Plaintiff Stacho's Private Information before, during and after the Data Breach.

237. Plaintiff Stacho reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Stacho would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

238. In a letter dated April 7, 2025, Defendant sent Plaintiff Stacho a notice letter informing him that his Private Information was compromised in the Data Breach.

239. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Stacho faces, Defendant offered victims of the Data Breach a temporary subscription to a credit monitoring service via the notice letter sent to impacted individuals.

240. Plaintiff Stacho greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Stacho is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

241. Plaintiff Stacho stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

242. As a result of the Data Breach, Plaintiff Stacho has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Stacho spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

243. As a consequence of and following the Data Breach, Plaintiff Stacho has experienced an uptick in spam calls, text messages, and emails.

244. The Data Breach has caused Plaintiff Stacho to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing his of the fact

that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

245. Plaintiff Stacho anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Stacho will continue to be at present and continued increased risk of identity theft and fraud for years to come.

246. Plaintiff Stacho has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

247. As a direct and traceable result of the Data Breach, Plaintiff Stacho suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private

Information, a form of intangible property that Defendant obtained from Plaintiff Stacho and (g) other economic and non-economic harm.

iii. Plaintiff Preston Tilger

248. Plaintiff Preston Tilger is unsure how Defendant obtained his Private Information, however, on information and belief, Defendant obtained and maintained Plaintiff Tilger's Private Information from his current or former employer. And as a result, Plaintiff Tilger was injured by the Data Breach.

249. Plaintiff Tilger (or his third-party agent) entrusted his Private Information to Defendant and trusted that Defendant would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Tilger's Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

250. Plaintiff Tilger (or his third-party agent) reasonably understood that a portion of the funds paid to Defendant for services would be used to pay for adequate cybersecurity and protection of Private Information.

251. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff Tilger's PII, including at least his full name, address, date of birth, and Social Security number. And upon information and belief, Plaintiff

Tilger's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

252. Plaintiff Tilger fears for his personal financial security and worries about what information was exposed in the Data Breach.

253. Because of the Data Breach, Plaintiff Tilger has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Tilger's injuries are precisely the type of injuries that the law contemplates and addresses.

254. Plaintiff Tilger suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

255. Plaintiff Tilger suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant were required to adequately protect.

256. Plaintiff Tilger suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Tilger's Private Information right in the hands of criminals.

257. Indeed, following the Data Breach, Plaintiff Tilger began experiencing a substantial increase in spam and scam text messages and phone calls, including messages about insurance (which Defendant provide to businesses), suggesting that his Private Information has been placed in the hands of cybercriminals.

258. On information and belief, Plaintiff Tilger's phone number was also compromised as a result of the Data Breach, as cybercriminals are able to use an individual's Private Information that is accessible on the dark web, to gather and steal even more information.

259. Because of the Data Breach, Plaintiff Tilger anticipates spending considerable amounts of time and money to try and mitigate his injuries.

260. Today, Plaintiff Tilger has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

261. As a direct and traceable result of the Data Breach, Plaintiff Tilger suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity

thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Tilger and (g) other economic and non-economic harm.

iv. Plaintiff Arthur Wagner

262. Plaintiff Arthur Wagner is a customer of Defendant and entrusted his Private Information to Defendant to obtain services for himself.

263. Thus, Defendant obtained and maintained Plaintiff's Private Information. As a result, Plaintiff Wagner was injured by Defendant's Data Breach.

264. Plaintiff Wagner entrusted his Private Information to Defendant and trusted that Defendant would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Wagner's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

265. Plaintiff Wagner reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

266. Plaintiff Wagner is very careful about sharing his sensitive Private Information . He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Wagner also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

267. In a letter dated April 7, 2025, Defendant sent Plaintiff Wagner a notice letter informing him that his Private Information was compromised in the Data Breach.

268. Thus, on information and belief, Plaintiff Wagner's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

269. Through its Data Breach, Defendant compromised Plaintiff Wagner's name and Social Security Number.

270. Plaintiff Wagner has already spent much time monitoring his account to protect himself and will continue to spend significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Wagner to take those steps in its Notice of Data Breach.

271. Plaintiff Wagner fears for his personal financial security and worries about what information was exposed in the Data Breach.

272. Because of Defendant's Data Breach, Plaintiff Wagner has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Wagner's injuries are precisely the type of injuries that the law contemplates and addresses.

273. Plaintiff Wagner suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

274. Plaintiff Wagner suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

275. Plaintiff Wagner suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Wagner's Private Information right in the hands of criminals.

276. Because of the Data Breach, Plaintiff Wagner anticipates spending considerable amounts of time and money to try and mitigate his injuries, including to continue to monitor his financial accounts.

277. Plaintiff Wagner maintains a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

278. As a direct and traceable result of the Data Breach, Plaintiff Wagner suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Wagner and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

279. Plaintiffs bring this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(2)&(3).

280. Plaintiffs propose the following nationwide class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information may have been compromised in the October 9, 2024 Data Breach, consisting of all individuals who received a Notice Letter (the "Class").

281. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

282. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

283. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

284. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief Defendant has knowledge of the number of individuals whose Private Information was compromised in Data Breach. Plaintiffs estimate that the Class is comprised of thousands of Class

Members, if not more. Further, Defendant has provided notice to HHS that 40,177 individuals were affected. Thus, the Class is sufficiently numerous to warrant certification.

285. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

f. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

g. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

h. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

i. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was per se negligent;

m. Whether Defendant failed to provide notice of the Data Breach promptly;

n. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

o. Whether Defendant took sufficient steps to secure individuals' Private Information;

p. Whether Defendant breached third-party beneficiary contracts for adequate data security with Class Members;

q. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Class Members;

r. Whether Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief; and

s. The nature of relief, including damages and equitable relief, to which Plaintiffs and Class Members are entitled.

286. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant and the same unreasonable manner of notifying individuals about the Data Breach. Plaintiffs are advancing the

same claims and legal theories on behalf of themselves and all other Class Members, and no defenses are unique to Plaintiffs. Plaintiffs' claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

287. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' interests do not conflict with Class Members' interests. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

288. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

289. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have

no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member. Thus, prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

290. The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiffs are not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

291. Information concerning Defendant's policies is available from Defendant's records.

292. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

293. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

294. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

295. Likewise, particular issues are appropriate for certification pursuant to Federal Rule of Civil Procedure 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard its clients' employees' Private Information; and

f. Whether adherence to FTC data security guidelines and/or measures recommended by data security experts would have reasonably prevented the Data Breach.

296. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified by Defendant.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

297. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

298. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

299. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

300. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

301. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals

whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

302. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access; and

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

303. Also, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

304. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

305. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

306. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third party agents) entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment and Defendant's services.

307. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

308. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs' and Class Members' and the importance of exercising reasonable care in handling it.

309. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

310. Defendant breached these duties as evidenced by the Data Breach.

311. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

312. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

313. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

314. Defendant admitted that the PII of Plaintiffs and the Class was accessed by an intruder to its systems.

315. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

316. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

317. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

318. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

319. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive Private Information.

320. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

321. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant's had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

322. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

323. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

324. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew

or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

325. Defendant's violations and its failure to comply with applicable laws and regulations constitute negligence *per se*.

326. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

327. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

328. Defendant offered to provide services on behalf of Plaintiffs and members of the Class (or their third-party agents) if, and in exchange, Plaintiffs and members of the Class entrusted Defendant with their Private Information.

329. In turn, Defendant agreed it would not disclose the Private Information it collects to unauthorized persons.

330. Plaintiffs and the members of the Class (or their third-party agents) accepted Defendant's offer by providing Private Information to Defendant in exchange for Defendant's services.

331. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

332. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

333. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Private Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

334. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

335. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

336. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

337. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

338. Defendant failed to send Notice to the victims promptly and sufficiently.

339. In these and other ways, Defendant violated its duty of good faith and fair dealing.

340. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

341. Plaintiffs, on behalf of themselves and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future

monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

342. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

343. This claim is pleaded in the alternative to the breach of implied contract claim.

344. Plaintiffs and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their Private Information to facilitate its business, and (2) from accepting payment for services it provided to Plaintiffs and the Class.

345. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members (or their third-party agents).

346. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

347. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information.

348. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

349. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' payment because Defendant failed to adequately protect their Private Information.

350. Plaintiffs and Class members have no adequate remedy at law.

351. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

352. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

353. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class

members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

354. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

355. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

356. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Private Information.

357. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

358. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SIXTH CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and Class Members)

359. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

360. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide employee benefit services, which included data security practice, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

361. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. This, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

362. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

363. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

364. As foreseen, Plaintiffs and Class Members were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the file sin its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

365. Accordingly, Plaintiffs and the Class are entitled to damages in the amount to be determined at trial, along with costs and attorneys; fees incurred in this action.

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

366. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

367. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

368. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations and Privacy Policy. Defendant's disclosure of Plaintiffs' Private Information is highly offensive to the reasonable person.

369. Defendant owed a duty to Plaintiffs and Class Members to keep their PII confidential.

370. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII, is highly offensive to a reasonable person. It constitute an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

371. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

372. Defendant's failure to protect Plaintiffs' and Class Members' Private Information acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

373. Defendant knowingly did not notify Plaintiffs' and Class Members in a timely fashion about the Data Breach.

374. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

375. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiffs and the Class Members was stolen by a third party and is

now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

376. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

377. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their Private Information. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

378. Plaintiffs and Class Members seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information.

379. Plaintiffs and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

380. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

381. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information that Plaintiffs and Class Members entrusted to Defendant.

382. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class was governed by terms and expectations that Plaintiffs' and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

383. Plaintiffs and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

384. Plaintiffs and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

385. Defendant voluntarily received Plaintiffs' and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

386. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

387. As a direct and proximate cause of Defendant's actions and omissions, Plaintiffs and the Class have suffered damages.

388. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information as well as the resulting damages.

389. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and Class Members' Private Information.

390. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer

injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

391. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

EIGHTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

392. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

393. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

394. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

395. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

396. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

397. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

398. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class Members' injuries.

399. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

400. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

401. WHEREFORE, Plaintiffs individually and on behalf of all others similarly situated, prays for judgment as follows:

a. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing her counsel to represent Class Members;

b. Awarding Plaintiffs and Class Members damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

c. Awarding restitution and damages to Plaintiffs and Class Members in an amount to be determined at trial;

d. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

e. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and Class Members;

f. Awarding attorneys' fees and costs, as allowed by law;

g. Awarding pre- and post-judgment interest, as provided by law;

h. Granting Plaintiffs and Class Members leave to amend this complaint to conform to the evidence produced at trial; and

i. Any and all such relief to which Plaintiffs and Class Members are entitled.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: June 12, 2025

Respectfully submitted

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Interim Class Counsel for Plaintiffs and the Proposed Class

Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Leigh S. Montgomery
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Telephone: (888) 350-3931

E. Powell Miler (P39487)
Gregory A. Mitchell (P68723)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Ste. 300
Rochester, MI 48307
(248) 841-2200
epm@millerlawpc.com
gam@millerlawpc.com

Gary M. Klinger
MILBERG COLEMAN PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
T: 866.252.0878
gklinger@milberg.com

Nathan J. Fink
FINK BRESSACK
38500 Woodward Ave., Suite 350
Bloomfield Hills, MI 48304
Telephone: (248) 971-2500
nfink@finkbressack.com

Sean Short
Arkansas Bar No. 2015079
SANFORD LAW FIRM, PLLC
Kirkpatrick Plaza
10800 Financial Centre Pkwy, Suite 510
Little Rock, Arkansas 72211
Telephone: (800) 615-4946
sean@sanfordlawfirm.com

Additional Plaintiffs' Counsel

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on June 12, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record, below, via the ECF system.

DATED this 12th day of June, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109